Australian National University

Procedure: Passwords

程序：密码

Purpose

目的

The University provides access to information infrastructure and services to authorised users within the University community. Passwords are the primary means of authenticating user access to ANU information services and systems. This procedure establishes the minimum standards for University system passwords and/or passphrases, and outlines their correct use.

本校为本校社区内授权用户提供对信息基础设施和服务的访问权。密码作为主要授权方式以便用户访问澳国立信息服务和系统。该程序为大学系统密码和/或密码短语建立最低标准，以及概述其正确使用方法。

Definitions

定义

Definitions of terms used in this document are provided in the overarching Information technology security policy.

《信息技术安全政策》概述了本文件中使用的术语的定义。

Standard users: those users who do not have privileged or elevated access to University systems, as defined in the Information technology account management and access procedure.

标准用户：指那些不具有《信息系统账户管理和准入程序》中定义的大学系统特权或高级访问权限的用户。

Procedure

程序

1. ANU is committed to ensuring appropriate security for all information technology, data, equipment, and processes within its domain of ownership and control.

   澳国立承诺在其所有权和控制权范围内确保所有信息技术，数据，设备和流程的适当安全性。

2. The University provides access for all:

   本校向以下所有用户提供访问权限：

   a. authorised users within the University community; and

      本校社区内的授权用户；以及

   b. network connecting devices authorised for connection, and that have been allocated an IP address within the University's IP Address range.

      已获得联通授权的，并且已获得本校 IP 地址序列内的 IP 地址的网络连接设备。

3. Suspected or known security incidents must be reported to the ITS Cyber and Digital Security Team by emailing it.security@anu.edu.au and remediation is coordinated from that office.

   如有发现疑似或已知的安全事件，须通过电子邮件将其报告给信息技术服务(ITS)网络和数字安全部门: it.security@anu.edu.au，并由该部门协调补救措施。

4. The use of the term password(s) in this document also includes passphrases(s).

   该文件中所使用的“密码”术语同样包含“密码短语”的意思。

University responsibilities

本校责任

5. The University is responsible for:

   本校负责：

a. providing and maintaining access to systems and resources for authorised users;

为授权用户提供系统和资源的访问权并进行维护；

b. suspending any part of an authorised user's access as a result of a security concern or policy breach, resulting from penalties or disciplinary action; and

如有授权用户受到处罚或纪律处分，进而引起安全性问题或有违政策，本校将暂停其任何访问权；以及

c. maintaining and amending minimum password standards as appropriate, to reflect current IT security protocols.

适当地维护和修改最低密码标准，以符合当前的信息技术安全协议。

User responsibilities

用户责任

6. Users:

用户：

a. observe and comply with all relevant policies and procedures;

遵守并服从所有相关政策和程序；

b. do not disclose their password to anyone else under any circumstances; and

在任何情况下，不向其他任何人泄露其密码；以及

c. do not allow any other individual access to a service or resource authenticated with their credentials

不允许其他个人访问其登录权限下可访问的服务或资源。

7. Passwords used for University systems are not reused for other systems or services.

不在其它系统和服务上重复使用大学系统密码。

8. User passwords are changed in accordance with the published account management standards for the system/service that they are accessing.

根据所访问的系统/服务的官方帐户管理标准，进行用户密码更改。

9. Passwords believed to have been compromised are changed immediately and the matter is reported by the user to the ITS Cyber and Digital Security Team by emailing it.security@anu.edu.au, in accordance with the Information technology security policy. In this event staff members also notify their supervisor.

   根据《信息技术安全政策》，如果怀疑密码已泄露，需要立即更改，并通过电子邮件将其报告给 ITS 网络和数字安全部 it.security@anu.edu.au。在这种情况下，工作人员还需通知其主管。

10. If a user wishes to record and store passwords, the following measures are undertaken:

    用户如果需要记录或保存密码，可以采取以下方式：

    a. records in hard copy are stored in a locked drawer, cabinet, room or area where access is controlled or has sufficient access control measures; and

       保存在纸质版本的记录需要存储在上锁的抽屉、橱柜、房间或访问可控或者具有足够的访问控制措施的区域；以及

    b. records in electronic format are stored on a system that requires user authentication.

       电子版本的记录需要存储在需要用户验证的系统中。

System owner responsibilities

系统所有者的职责

11. System owners enforce the minimum password standards set out in this document when allowing user access to the systems under their ownership.

    系统所有者在允许用户访问其权限内的系统时，需强制执行该文件中规定的最低密码标准。

12. System owners of systems containing sensitive or highly sensitive data:

    含有敏感或高度敏感数据系统的系统所有者：

a. may heighten authentication requirements in line with the Enterprise systems management standard; and
在符合《企业系统管理标准》的前提下，可以提高身份验证要求；以及

b. publish heightened authentication requirements to users of that system directly at the time the account is issued and at least annually thereafter.
在生成帐户时，直接向该系统的用户发布更高的身份验证要求，并且此后至少每年一次。

Minimum password standards

最低密码标准

13. Standard user passwords meet the following requirements. Passwords:
标准用户密码需要满足以下要求。密码：

a. are a minimum of 10 characters;
至少含有 10 个字符；

b. include at least one character from each of at least three of the following groups:
从以下三组字符的每组中，包含至少一个字符：

- lowercase characters (a - z)
  小写字母(a - z)
- uppercase characters (A – Z)
  大写字母(A – Z)
- digits (0 - 9)
  数字(0 - 9)
- punctuation and special characters ($, !, %, ^, (,), {, }, [,], ;, :, <, >, ?)
  标点符号和特殊符号($, !, %, ^, (,), {, }, [,], ;, :, <, >, ?)
- unicode characters; and
  统一码 (unicode) 字符；并且

c. do not consist of:
不能含有：

- the account name in any form (as-is, reversed, capitalised, doubled, etc.);

  任何形式的账户名（原样复制，倒序，大写，加倍等）；

- the user’s first or last name in any form;

  任何形式的用户的名字或姓;

- simple patterns of letters on keyboards; or

  键盘上简单排列的字母；或者

- any well-known or publicly posted identifiable information.

  任何知名或公开发布的可识别信息。

Initial and reset password generation

生成初始密码和重置密码

14. All initial and assisted reset passwords are generated randomly.

    所有初始密码和辅助重置密码都是随机生成的。

15. Requests for user password resets require suitable proof of identity before being actioned. Suitable proof of identity for password resets include:

    处理用户密码重置请求之前，需要适当的身份验证。密码重置的合适身份证明包括：

    a. photo ID;

       有照片的证件;

    b. supervisor identification; or

       主管身份验证；或

    c. satisfactory challenge-responses.

       符合要求的验证答复。

16. All password resets generate an auditable log indicating at a minimum the date, time, account name, and who conducted the reset.

    所有密码重置都会生成一个可审核的日志，该日志至少包含：日期，时间，帐户名和重置者。

17. Password resets conform to the same controls as set out for initial password generation.

密码重置时遵循与初始密码生成相同的管制。

18. User passwords are only recorded upon initial generation. Only one copy is made and this is provided directly to the owner of the password.

    用户密码仅在初始生成时有记录。该记录仅生成一份，并直接提供给密码所有者。

19. User passwords are not disclosed to anyone other than the password owner under any circumstances.

    在任何情况下，都不可将用户密码透露给密码所有者以外的任何人。

20. Group passwords are discouraged. Where no alternative exists, group passwords can:

    不建议使用群组密码。如果没有其他选择，群组密码可以：

    a. only be disclosed to individuals who have been authorised to access a particular electronic resource or service as part of that group.

       仅透露给授权个人用来访问特定群组内的电子资源或服务。

    a. be changed whenever a member of the group leaves the group or at least as often as a user password.

       在群组成员离开该群组时进行更改或至少像用户密码一样经常进行更改。

Identity self service portal

身份自助服务门户

21. Some systems utilise the Identity Self Service Portal (ISSP) to generate and manage passwords. The following apply to passwords generated and managed in this manner.

    某些系统利用身份自助服务门户（ISSP）生成和管理密码。以下内容适用于以这种方式生成和管理的密码。

22. The initial password is valid for 14 days, after which it will expire.

    初始密码有效期为 14 天，之后将失效。

23. When issued with an initial password, users change the issued password immediately by:

    初始密码发出后，用户可以通过以下方式立即更改发出的密码：

    a. logging into the Identity Self Service portal;

       登录身份自助服务门户；

    b. reading the required ANU policies; and

       阅读必要的澳国立政策；并且

    c. setting up security questions and answers.

       设置安全问题和答案。

24. All passwords created using the ISSP have a minimum lifespan of 24 hours. A user can not change their password again during this period, except via an assisted password reset.

    使用 ISSP 创建的所有密码的最小时限为 24 小时。在此期间，用户无法再次更改其密码，除非通过辅助密码重置装置。

25. All passwords created using the ISSP have an expiry period of 180 days.

    使用 ISSP 创建的所有密码的有效期为 180 天。

26. Users receive an automatic email notification after a password reset has occurred.

    密码重置后，用户会收到一封自动生成的电子邮件通知。

27. Users cannot use any of the previous five passwords when setting a new password.

    设置新密码时，用户无法使用之前使用过的五个密码中的任何一个。

28. An assisted password reset provides the user with a temporary password to be used only once to log in to the ISSP. This password is valid for 24 hours only, after which the password will expire.

    辅助密码重置为用户提供一个临时密码，该密码只能用于登录 ISSP 一次。该密码仅在 24 小时内有效，此后密码将过期。

29. After a password has expired, users are still able to log into the Identity Self Service portal to reset their passwords.

密码过期后，用户仍然可以登录到身份自助服务门户进行密码重置。

Translated on 4 March 2021

Source https://policies.anu.edu.au/ppl/document/ANUP_013008